

中华人民共和国国家标准

GB/T XXXXX—202X

人工智能 政务大模型系统技术要求

Artificial intelligence—Technical requirements for large scale model system of
government affairs

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布

XXXX-XX-XX 实施

国家市场监督管理总局
国家标准化管理委员会

发布

目 次

前言III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 系统参考架构 2

6 政务大模型能力要求 3

 6.1 语义理解 3

 6.2 长文本理解 4

 6.3 图像分类 4

 6.4 内容生成 4

 6.5 文本问答 5

 6.6 音频问答 5

 6.7 多模态处理 5

7 应用支撑要求 5

 7.1 数据工程 6

 7.2 训练微调 6

 7.3 提示词工程 7

 7.4 智能体开发管理 7

8 场景应用要求 7

 8.1 政务服务 7

 8.2 社会治理 9

 8.3 机关办公 9

 8.4 辅助决策 10

9 安全合规要求 11

 9.1 基本要求 11

 9.2 数据安全要求 11

 9.3 模型和系统安全要求 12

 9.4 内容生成安全要求 12

 9.5 监管审核要求 12

10 部署运维要求 12

 10.1 系统部署 12

 10.2 运维工具 12

 10.3 模型管理 13

 10.4 系统管理 13

11 非功能性要求 13

 11.1 可靠性要求 13

11.2 兼容性要求13

11.3 维护性要求13

参考文献15

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、人民法院信息技术服务中心、华为技术有限公司、河南省政务大数据中心、北京市大数据中心、华中科技大学、湖南农业大学、浪潮云信息技术股份公司、拓维信息系统股份有限公司、福建省人民政府办公厅电子政务中心、北京华宇信息技术有限公司、大汉软件股份有限公司、北京理工大学、北京海纳数聚科技有限公司、山西远大纵横科技有限公司、北京中百信信息技术股份有限公司、阿里云计算有限公司、中电科大数据研究院有限公司、北京兴云数科技术有限公司、昆仑数智科技有限责任公司、武汉金山办公软件有限公司、北京百度网讯科技有限公司、华为云计算技术有限公司、北京金山办公软件股份有限公司、广电运通集团股份有限公司、国投智能信息科技股份有限公司、华信咨询设计研究院有限公司、讯飞智元信息科技有限公司、中移雄安信息通信科技有限公司、中国经济信息社有限公司、人民中科（北京）智能技术有限公司、新华三技术有限公司、浙江省质量科学研究院、智慧足迹数据科技有限公司、福昕鲲鹏（北京）信息科技有限公司、北京华电园信息技术有限公司、无锡市市域社会治理现代化指挥中心、数集（青海）科技有限公司、上海金桥信息股份有限公司、华中师范大学、以萨技术股份有限公司、云赛智联股份有限公司、量安科技（北京）有限公司、南京安通杰科技实业有限公司、北京致远互联软件股份有限公司、南京安夏电子科技有限公司、永中软件股份有限公司、中科信控（北京）科技有限公司、可码科技（江苏）有限公司、园测信息科技股份有限公司、四川极速动力科技有限公司、进迭时空（杭州）科技有限公司、江西微博科技有限公司、中国口岸协会口岸科技应用分会、湖南科创信息技术股份有限公司。

本文件主要起草人：王雷、王晓燕、相福民、于浩、崔昊、彭革非、顾晓光、陈璐、陈涛、林文河、明承瀚、郑佳佳、赵江涛、康丽丽、金震宇、王树良、张旭、孙传兴、胡璐锦、卢学哲、何运昌、曹扬、刘海军、尚云云、包树南、张英博、郑子木、闫石、吴涛、冯晓蒙、杨旭、阙锦龙、赵学健、陈士星、郑庆国、杨光、秦晓鲁、万晓兰、章古月、施含章、张治、董艳会、杜巍、段尧清、章建兵、钟军、陈豪、龙江涛、梁勇、王翔、杨庄媛、张宏、冯健、武传营、徐浩天、谷敏骏、齐勇、周传健、钱程扬、张小刚、涂震、方明。

人工智能 政务大模型系统技术要求

1 范围

本文件确立了政务大模型系统的参考架构，规定了政务大模型系统的模型能力、应用支撑、场景应用、安全合规、部署运维和非功能性等要求。

本文件适用于政务大模型系统的设计和开发，也可为政务大模型测评提供指导。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 4657 中央党政机关、人民团体及其他机构代码
- GB/T 21063.4—2007 政务信息资源目录体系 第4部分：政务信息资源分类
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 25647—2010 电子政务术语
- GB/T 32905 信息安全技术 SM3密码杂凑算法
- GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法
- GB/T 32907 信息安全技术 SM4分组密码算法
- GB/T 36464.3—2018 信息技术 智能语音交互系统 第3部分：智能客服
- GB/T 39554.1—2020 全国一体化政务服务平台 政务服务事项基本目录及实施清单 第1部分：编码要求
- GB/T 41867—2022 信息技术 人工智能 术语
- GB/T 45288.1—2025 人工智能 大模型 第1部分：通用要求
- GB/T 45396 数据安全技术 政务数据处理安全要求
- GB 45438—2025 网络安全技术 生成式人工智能合成内容标识方法
- GB/T 45654—2025 网络安全技术 生成式人工智能服务 安全基本要求
- GB/T 45674 网络安全技术 生成式人工智能数据标注安全规范
- GA/T 2380 信息安全技术 网络安全等级保护数据安全基本要求

3 术语和定义

GB/T 41867—2022界定的以及下列术语和定义适用于本文件。

3.1

大模型 large-scale model

基于大量数据训练得到，具有复杂计算架构，能处理复杂任务，且具备一定泛化性的深度学习模型。

[来源：GB/T 45288.1—2025，3.1]

3.2

政务大模型 large-scale model of government affairs

基于政务数据和业务逻辑，对基础大模型进行训练、微调形成的，适配政务领域场景需求的深度学习模型。

注：政务领域应用通常采用参数高效的微调技术手段。

3.3

政务大模型系统 large-scale model system of government affairs

以政务大模型为核心，具备为政务服务、社会治理、机关办公、辅助决策等提供人工智能辅助服务的系统。

3.4

政务数据 government data

各级政务部门及其技术支撑单位在履行职责过程中依法采集、生成、存储、管理的各类数据资源。

注：根据可传播范围，政务数据一般包括可共享政务数据、可开放公共数据及不宜开放共享政务数据。

[来源:GB/T 38664.1—2020, 3.1]

3.5

语义理解 semantic comprehension

本文件特指理解政务领域专业术语、政策文件结构、业务流程，以及典型用户需求表达，并按照要求输出正确反馈结果的过程。

[来源:GB/T 36464.3-2018, 3.6, 有修改]

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

API：应用程序编程接口（Application Programming Interface）

DPO：直接偏好优化（Direct Preference Optimization）

GPU：图形处理器（Graphics Processing Unit）

GRPO：分组相对策略优化（Group Relative Policy Optimization）

LoRA：低秩适应（Low-Rank Adaptation）

MCP：模型上下文协议（Model Context Protocol）

MTP：多词元预测（Multi-Token Prediction）

PD：预填充解码（Prefill Decode）

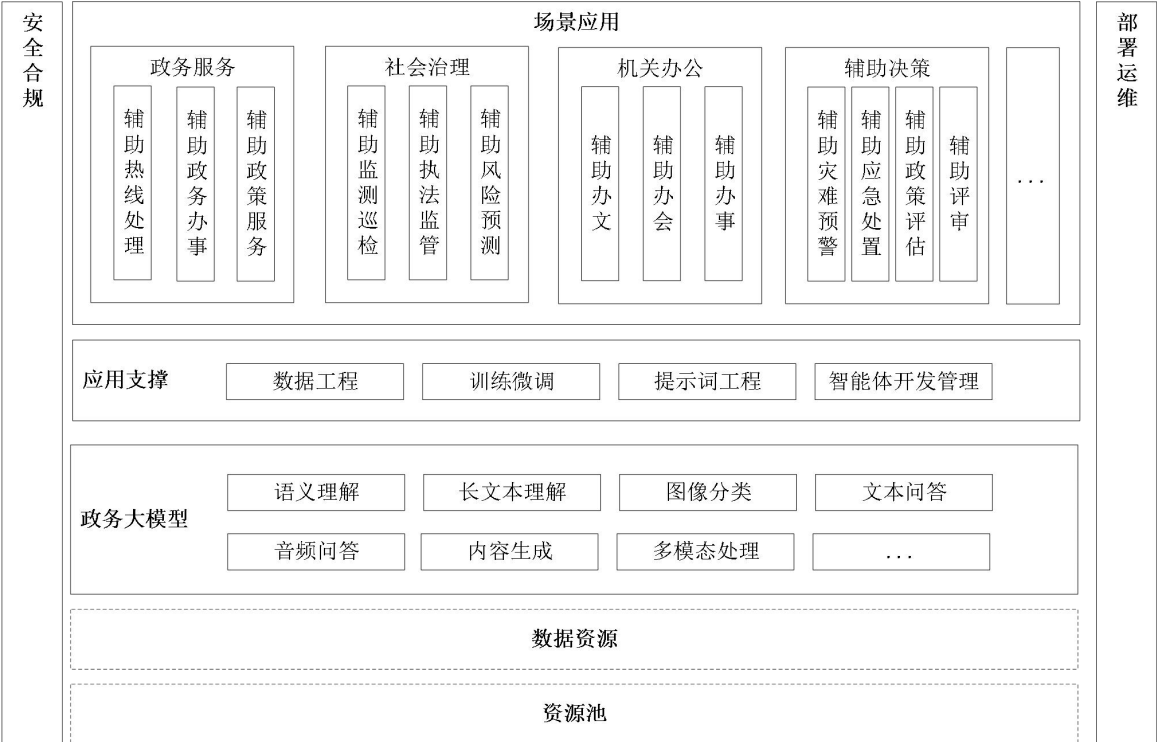
OFD：开放版式文档（Open Fixed layout Document）

SFT：监督微调（Supervised Fine-Tuning）

UOF：统一办公文档格式（Uniform Office Document Format）

5 系统参考架构

政务大模型是政务大模型系统中的核心组成部分，具备满足政务领域应用需求的语义理解、长文本理解、图像分类等能力。按照GB/T 45288.1—2025第4章规定的大模型参考架构，结合政务领域应用实际，政务大模型系统参考架构由资源池、数据资源、政务大模型、应用支撑、场景应用、安全合规和部署运维等七个部分构成，如图1所示。



注：图中虚线部分仅表明是政务大模型系统的相关组成部分，本文件不对其提出具体要求。

图 1 政务大模型系统参考架构

- 政务大模型系统各组成部分及交互关系如下：
- 资源池为上层模块提供基础设施能力支撑，主要包括计算资源、存储资源和网络资源等；
 - 数据资源是从各类政务业务系统和公共资源中采集的，用于训练、微调的数据集，以及训练、微调后形成的政务知识库；
 - 政务大模型是政务大模型系统的核心组成，具备支撑政务场景应用的语义理解、长文本理解、图像分类等共性基础能力，应符合第 6 章的规定；
 - 应用支撑通过数据工程、训练微调、提示词工程等调用政务大模型能，以支撑政务场景应用，应符合第 7 章的规定；
 - 场景应用为各类政务业务系统提供场景化、智能化赋能服务，向下对接模型与服务的核心能力，向上直接承载政务领域的业务需求。场景应用主要包括政务服务、社会治理、机关办公、辅助决策等方面。政务大模型系统根据应用实际，可灵活配置场景应用。相关场景应用应符合第 8 章的规定；
 - 安全合规负责对全流程数据流和操作行为进行管控，应符合第 9 章的规定；
 - 部署运维负责系统的全生存周期管理，应符合第 10 章的规定。
- 此外，政务大模型系统的非功能性要求应符合第 11 章的规定。

6 政务大模型能力要求

6.1 语义理解

语义理解能力在语法分析、语义处理、综合理解等方面，应至少符合以下要求：

- a) 句子分词：具备识别政务领域专用词汇的能力，涵盖内容至少包括 GB/T 25647—2010 第 3 章规定的术语，GB/T 4657 规定的机构名称与简称，以及政务领域相关主题词和复合词等；
- b) 词性标注：具备赋予政务领域的专用词汇词性的能力；
- c) 语法分析：具备解析政务领域文本的核心成分关系、句式结构和修饰逻辑的能力；
- d) 语义角色标注：具备标注政务领域文本中谓词和论元的语义角色的能力；
- e) 信息抽取：具备提取政务领域文本中的事实、实体和关系等的的能力；
- f) 任务分类：具备根据用户输入内容，将其匹配至所属政务任务类目的能力；
- g) 语义分析与推理：具备识别用户意图，进行政策逻辑推理、常识推理的能力；
- h) 情感分析：具备识别文本所表达的情绪状态（如满意、不满、焦急、平静等）的能力；
- i) 指代消解与关联：具备辨识“本、该、此、相关、有关”等政务领域常用代词，以及复现短语的具体指代对象的能力，能在后续语义理解与内容生成中保持指代关系一致；
- j) 上下文记忆：具备留存和调用多轮对话中具有政务领域特色关键信息的能力。

6.2 长文本理解

长文本理解能力从整体、局部到全局等方面，应至少符合以下要求：

- a) 解析对象：长文本包括但不限于法律法规、政策文件、电子公文、电子档案等；
- b) 结构解析：具备解析内容层级结构、输出结构化框架的能力；

示例：公文主体始于标题，公文版记一般始于“抄送：”。

- c) 要素识别：具备提取关键概念的能力，如责任主体、政策条款、适用范围、时限要求、奖惩规则、政策依据等；
- d) 逻辑分析：具备识别对象逻辑关系的能力，如政策沿革、事件发展、因果逻辑等；
- e) 跨文档信息处理：具备对相关关联的多份长文本进行版本异同比对、上位法与下位法条款对应分析、跨部门政策衔接关系分析等能力；
- f) 一致性检查：具备内容表述一致性的检查能力。

6.3 图像分类

图像分类能力应至少符合以下要求：

- a) 特征识别：具备识别并提取政务高频应用中图像语义信息的能力，如电子印章、公文标题、巡查问题类型、个人隐私信息等；
- b) 类别判断：具备基于图像核心要素标签进行图像分类、注明分类依据的能力；
- c) 安全处置：具备图像敏感信息的识别能力，能提示相关风险并触发处置措施。

6.4 内容生成

内容生成能力在基础生成、生成控制、生成管理等方面，应至少符合以下要求：

- a) 生成加工：具备生成符合政务服务、社会治理、机关办公、辅助决策等应用场景需求，且具备特定格式要求的单一模态或多模态内容的能力；
- b) 指令控制：具备根据用户指令（如正式书面、简洁严谨、通俗易懂等），调整写作风格、内容长度、排版格式等能力；
- c) 摘要总结：具备从电子公文、法律法规、政策文件等长文本中提取关键信息并生成摘要内容的能力；
- d) 多语种处理：具备将汉语与英语、法语等政务对外交流高频语种进行互译及生成的能力，译文准确传达政务术语含义；

- e) 数据类型：具备根据输入指令，生成结构化与非结构化数据格式的能力，至少支持 UOF、OFD 等文档格式；
- f) 生成依据：具备在生成内容中标明推理依据或原文出处的能力；
- g) 内容标识：具备在生成的文本、图片中，添加显式标识或隐式标识的能力，标识应符合 GB 45438 规定；
- h) 脱敏处理：具备对生成内容中的敏感信息进行脱敏处理的能力。

6.5 文本问答

文本问答能力应至少符合以下要求：

- a) 问题理解：具备 6.1 和 6.2 规定的的能力；
- b) 问题应答：具备根据文本问题提供准确的答案或相关信息能力，相关能力应符合 6.4 的规定；
- c) 有据可查：具备在输出的文本回答内容旁，以角标等方式标明推理依据或原文出处的能力。对于暂无明确依据的，提示内容由人工智能生成合成；
- d) 多轮对话：具备跟踪会话内上下文的能力，能基于历史交互推断用户真实意图并自动调整回答策略。对于表述模糊的问题，能主动发起追问引导，以明确用户诉求；
- e) 应答处理：具备配置政务场景常用应答模板和分级响应的能力。对于简单问题，调用模板自动应答；对于复杂问题，结合知识推理生成定制化应答；对于疑难问题（包含用户意图表达不清或模型响应未达预期等问题），转接人工坐席应答并同步问答上下文；
- f) 会话管理：具备根据政务场景的会话需求，配置短期会话和长期会话的保留策略和清理方式的能力。能跨会话调用信息。

6.6 音频问答

音频问答能力应至少符合以下要求：

- a) 问题理解：具备 6.1 和 6.2 规定的的能力，具备识别汉语方言的能力，能适配低质量音频；
- 注：汉语方言通常包括官话方言、晋方言、吴方言、闽方言、客家方言、粤方言、湘方言、赣方言、徽方言、平话土话等。
- b) 情绪识别：具备识别音频所表达的情感状态；
 - c) 问题应答：根据语音输入的问题提供准确的答案或相关信息，相关能力应符合 6.4 的规定；
 - d) 多轮对话：具备跟踪多条语音上下文的能力，支持单会话内多条语音的意图连贯跟踪和跨会话语音的同一事项信息延续。

6.7 多模态处理

多模态处理能力在视觉单模态、语音单模态、跨模态交互等方面，应至少符合以下要求：

- a) 视觉识别：具备识别图像、视频中的核心信息的能力；
- b) 图像编辑：具备对图像进行修复、添加水印、图像补全等的的能力；
- c) 语音合成：具备将文本信息转化为语音的能力；
- d) 图像生成文本描述：具备根据图像生成文字描述信息的能力；
- e) 文本生成图像：具备通过文本指令生成对应语义图像的能力，支持泛化语义和多种风格；
- f) 图文文档理解：具备理解政务领域图文混排文档，整合文本与图表信息，生成摘要信息的能力；
- g) 图文检索：具备根据文本信息，检索相关图像文件的能力。

7 应用支撑要求

7.1 数据工程

7.1.1 数据标注

数据标注用于管理政务大模型训练微调所需的数据语料，应至少符合以下要求：

- a) 数据采集：具备文档、图像、音频、视频、数据库表等数据采集功能，支持UOF、OFD等文档格式，以及常见的图像、音频、视频文件格式；
- b) 数据标注：提供可视化的数据标注界面，具备对文本、图像等多模态政务数据的标注功能。其中，文本类政务数据支持序列标注（包含实体标注、语义角色标注）、关系标注等，图像类政务数据支持实体标注、关系标注等。具备基于机器学习模型的预标注功能；
- c) 标签管理：具备适用政务应用场景的标签分类管理功能；
- d) 任务管理：具备标注任务的管理功能，包括任务创建、任务分配、任务跟踪与结果审核等。

7.1.2 知识管理

知识管理用于整合、处理和利用政务大模型所需的数据资源，应至少符合以下要求：

- a) 数据接入：提供知识库开放接口，具备数据接入能力；
- b) 知识构建：具备基于UOF、OFD等非结构化数据以及结构化数据的知识构建功能，包括知识解析、清洗、政策时效性识别、知识单元拆分、知识图谱构建与管理等。具备按照业务领域、安全等级等维度进行知识分类管理功能；
- c) 知识检索：具备关键词检索、结构化条件检索、语义理解检索等功能；
- d) 知识库管理：具备挂载、更新、移除知识库插件功能；
- e) 知识运维：具备知识动态更新、版本控制、定期审查功能，具备政策文件有效性标记功能。

7.1.3 政务租户数据隔离管理

政务租户空间管理用于对政务大模型的租户、用户、权限和模型空间资源进行统一管理，应至少符合以下要求：

- a) 可视化的全维度隔离：具备可视化多租户管理功能，实现租户间空间资源、用户权限、模型资产的三级隔离；
- b) 资产的隔离与共享：具备模型资产、模型服务及第三方API资产在租户和空间维度的精细化隔离与共享控制能力；
- c) 租户的权限管控：具备用户与权限管理功能，包括但不限于用户管理、角色管理和授权管理。

7.2 训练微调

训练微调用于使大模型适配政务场景，应至少符合以下要求：

- a) 模型兼容：具备国内主流大模型的兼容能力，支持语言大模型和多模态大模型；
- b) 政务数据集管理：具备训练数据集的创建、版本管理及多方式接入（如文件、对象存储、高性能存储等）功能，支持对数据集进行质量校验与安全过滤；
- c) 模型训练：具备模型训练管理能力，支持对训练任务进行管理，包括训练任务超参配置、训练资源配置、训练任务详情查看、训练任务启用或停止、训练任务容错调度、训练任务故障恢复、训练任务核心指标可观测等，支持多种训练方法，包括监督微调（SFT）、低秩适应（LoRA）、直接偏好优化（DPO）、分组相对策略优化（GRPO）等；

注：SFT训练适用于基础政务知识植入，LoRA训练适用于轻量化定制化需求，DPO训练或GRPO训练适用于具体业务场景优化。

- d) 模型微调：使用高效参数微调技术进行模型微调，如增量微调、部分微调、重参数化等方法；

- e) 模型压缩：使用知识蒸馏、模型量化等能力，降低模型大小以适应存储和计算需求；
- f) 模型评估：具备模型评估管理功能，包括管理评测集、裁判模型、参评对象、评测任务管理、评测分析报告管理等，支持自动评估和人工评估模式；
- g) 模型推理：具备通过API等方式提供模型推理服务的能力，具体要求如下：
 - 1) 支持模型服务筛选、模型服务调试、模型服务详情、模型服务日志、模型服务流量控制等；
 - 2) 支持推理加速，如MTP推理加速、PD分离推理加速。

7.3 提示词工程

提示词工程应至少符合以下要求：

- a) 提示词模板新建：根据政务具体业务场景，选择上下文（任务的政策依据、适用范围等）、角色（模型的政务专属角色）、指令（待完成的具体政务任务）、风格（输出内容的表述风格）、受众（输出内容的目标受众）、输出（输出内容的格式、篇幅要求等）等要素或自定义配置提示词模板。

示例：上下文为“基于《××市××实施办法》（××发〔2025〕×号）”；角色为“政策解读助手”；指令为“解读某政策的申报条件和办理流程”；风格为“通俗化、口语化”；受众为“面向小微企业负责人”；输出为“分点列明，每点标注核心关键词，不超过 300 个字”。

- b) 提示词模板管理：具备提示词模板新建、查询、显示、编辑、调试、删除等功能。能配置提示词标签，辅助提示词模板的调用和查找；
- c) 提示词优化管理：能根据用户输入的提示词描述进行指令优化。具备提示词指令优化任务查看、终止、删除功能；
- d) 提示词评估：具备提示词评估功能，能从准确性、有效性、实用性、用户反馈等维度进行评估，并提供测试数据集和评估技术支撑。

7.4 智能体开发管理

智能体开发管理应至少符合以下要求：

- a) 开发方式：支持低代码、零代码及全代码等多种智能体开发方式；
- b) 功能配置包括以下方面：
 - 1) 规划配置：具备思考模式、思考次数等配置功能；
 - 2) 模型配置：具备模型的类型（如规划、生成等）、模型参数等配置功能；
 - 3) 记忆配置：具备长短期记忆的创建、编辑、删除等功能；
 - 4) 知识配置：具备政务数据的接入、调用调试、更新、调用策略管理、权限管理等功能；
 - 5) 工具配置：具备 API、MCP 等不同类型工具的注册、对接和调试功能，具备多工具调用结果的聚合、校验和反馈功能。
- c) 智能体互联：具备多智能体协同处理功能，包括知识共享、协同决策、冲突处理（如按优先级解决资源竞争）等；
- d) 智能体管理：具备智能体创建、编辑、删除等功能；
- e) 智能体运维：具备智能体评估、状态监控和调试等功能。

8 场景应用要求

8.1 政务服务

8.1.1 辅助热线处理

热线处理辅助应至少符合以下要求：

- a) 具备来电监测和分析功能，监测内容包括热点问题、高频诉求、异常来电等；
- b) 具备将普通话和汉语方言等语音转录为文本功能；
- c) 具备情感分析功能，并根据识别结果，推送应答模板和应对策略；
- d) 具备答案推荐、知识推荐、匹配度阈值配置等功能，匹配度计算基于语义相似度算法；
- e) 具备基于知识库服务，自动生成标准问答模版功能；
- f) 具备根据问题复杂度智能分配客服功能，能自动将疑难问题转接人工坐席处理；
- g) 具备表单字段自动填充功能，能根据咨询内容，以及合规读取用户历史办理数据，自动填充表单信息；
- h) 具备结合业务规则，对必填项、数据格式、逻辑关系等进行校验和错误提示功能；
- i) 具备工单摘要生成功能，自动标记需人工核验的内容；
- j) 具备工单自动派单与分流功能，基于问题类型、所属区域、办理权限等信息，自动推荐最优办理部门。

8.1.2 辅助政务办事

辅助政务办事包括办事引导、辅助申报、辅助审批、政务问数与分析等，具体如下：

- a) 办事引导应至少符合以下要求：
 - 1) 具备基于多轮会话和上下文关联，进行办事流程引导功能；
 - 2) 具备办事信息（如部门、步骤、材料等）生成与展示功能；
 - 3) 具备对复杂办事任务的拆解和分步骤指引功能；
 - 4) 具备搜问一体、热点服务个性化推荐等功能，快速定位需办理的事项。
- b) 辅助申报应至少符合以下要求：
 - 1) 具备基于问答和材料等内容提取要素、生成摘要，并自动填充表单字段功能；
 - 2) 具备在保障用户信息安全前提下，合规调取用户历史办事数据，自动填充表单字段功能；
 - 3) 具备依据业务规则，对填写内容、上传材料进行自动校验和错误提示功能。
- c) 辅助审批应至少符合以下要求：
 - 1) 具备自动识别审批要点，以及辅助生成审批要点与审批建议功能；
 - 2) 具备关联政策依据和信息来源功能；
 - 3) 具备提供相似历史案例的基本信息、审批结果和处理建议等功能，例如基于事项类型、申请条件、材料清单、审批结果等维度匹配相似案例；
 - 4) 具备智能标记异常事项、自动生成错误提示功能。
- d) 政务问数与分析应至少符合以下要求：
 - 1) 具备基于交互问答，对政务服务数据（如事项、办件、评价等）进行查询和统计功能，说明查询的数据源和统计口径；
 - 2) 支持以交互问答生成政务服务可视化分析图表和分析报告，报告中注明数据来源、时间范围等信息，并对生成的分析结论进行溯源。

8.1.3 辅助政策服务

辅助政策服务包括政策解读、政策匹配和政策兑现等方面，具体如下：

- a) 政策解读应至少符合以下要求：
 - 1) 具备政策内容的语义理解与分析功能，识别政策文件中的关键信息，如适用对象、标准、申报条件等；
 - 2) 具备政策摘要的生成功能；

- 3) 具备同一政策的版本管理、新旧条款差异对比等功能，具备政策关联网络的构建功能；
- 4) 具备用户咨询偏好与历史交互信息的存储功能，能基于用户需求提供个性化推荐。
- b) 政策匹配应至少符合以下要求：
 - 1) 具备企业信息画像的构建功能；
 - 2) 具备用户信息与政策要求的匹配功能；
 - 3) 具备生成符合政策要求的事项申报路径功能，包含时间节点、材料清单、受理部门等信息；
 - 4) 具备政策文件真实性核验功能，包括政策文号准确性、政策有效性状态等。
- c) 政策兑现应至少符合以下要求：
 - 1) 具备政策与受众群体智能匹配功能，向符合条件的用户主动推送政策解读、申报指南等信息；
 - 2) 具备政策兑现进度查询与节点提醒功能。

8.2 社会治理

8.2.1 辅助监测巡检

辅助监测巡检应至少符合以下要求：

- a) 具备多源异构数据接入与融合分析功能，分析视频监控、遥感影像、物联感知设备等数据，自动识别违规行为、设备故障、风险隐患等问题；
- b) 具备智能风险预警与辅助处置功能，生成并推送预警信息，并提供相关联的处置措施与管理建议；
- c) 具备巡检报告自动生成与巡检路径优化功能。

8.2.2 辅助执法监管

辅助执法监管应至少符合以下要求：

- a) 具备违法线索智能发现、追踪与评估功能；
- b) 具备执法依据、自由裁量基准和典型案例的智能推荐功能，根据违法事实、情节轻重自动匹配相应的法律条款与裁量标准；
- c) 具备执法文书的辅助生成与要素校验功能，根据案件信息辅助填充执法文书关键内容，对缺失项、逻辑矛盾等进行提醒；
- d) 具备案件报告自动生成功能；
- e) 具备执法过程智能监督与风险提示功能，开展执法过程合规性监督、案件质量评价与风险提示。

8.2.3 辅助风险预测

辅助风险预测应至少符合以下要求：

- a) 具备多源数据融合与风险推演预警功能，对风险开展监测、趋势推演与影响仿真，实现系统性、区域性风险的早期识别和预警；
- b) 具备重点对象潜在风险预测评估功能，基于历史数据与风险模型，对重点行业、关键领域、重要事项、关键人员等开展潜在风险概率预测与等级评估；
- c) 具备风险预警信息与应对建议的生成功能，自动生成风险预警信息，并提供风险溯源、影响评估与应对策略建议。

8.3 机关办公

8.3.1 辅助办文

辅助办文包括辅助公文起草、辅助公文改写、辅助公文审核和辅助公文排版，具体如下：

a) 辅助公文起草应至少符合以下要求：

- 1) 具备 15 种公文内容提纲和素材的辅助生成功能，包括结构框架、内容要点、规范句式、参考素材等；

注：《党政机关公文处理工作条例》规定的15个公文种类，包括决议、决定、命令（令）、公报、公告、通告、意见、通知、通报、报告、请示、批复、议案、函、纪要。

- 2) 具备基于现有结构和文风，生成相关参考内容功能，供公文起草者参考使用；

- 3) 具备生成全文或片段内容摘要、提炼标题等功能。

b) 辅助公文改写应至少符合以下要求：

- 1) 具备基于现有内容进行扩写、缩写、重写等功能；
- 2) 具备全文、片段、提纲的润色功能。

c) 辅助公文审校应至少符合以下要求：

- 1) 具备字词类、语法类、常识类和事件类错误校对功能，并给出纠正建议；
- 2) 具备内容查重功能，并给出修改建议；
- 3) 具备内容比对功能，呈现内容差异。

d) 辅助公文排版应至少符合以下要求：

- 1) 具备自动排版功能，完成排版的公文格式符合 GB/T 9704—2012 的规定；
- 2) 具备自动生成公文大纲功能，识别并设置段落结构和多层级标题，生成目录结构；
- 3) 具备排版样式的定制功能。

e) 辅助收文办理应具备收文表单自动填写功能，解析接收的电子公文，并将公文收发信息自动填充到收文处理单中：

8.3.2 辅助办会

辅助办会应至少符合以下要求：

- a) 具备会议材料生成和校核功能，包括会议议题、议程安排、参会人员等；
- b) 具备会议纪要生成功能，将会议音频转换成文本并提炼形成会议纪要；
- c) 具备会议纪要处理功能，包括摘要总结、关键词提取、观点提炼和工作任务梳理等。

8.3.3 辅助办事

辅助办事应至少符合以下要求：

- a) 具备提供动态指标分析与预测功能，自动分析趋势变化，模拟政策调整效果；
- b) 具备政策实施效果模拟功能，包括经济发展预测、群众投诉趋势、企业投资意愿等；
- c) 具备办理流程和相关文件的检索功能，通过输入的关键词，检索相关业务流程和所需文件；
- d) 具备专题资料的汇编功能；
- e) 具备识别电子公文或会议音频中的待办事项功能；
- f) 具备待办事项分解、智能提取关键信息、匹配办理部门、提交后续流程等功能。

8.4 辅助决策

8.4.1 辅助灾害预警

辅助灾害预警至少符合以下要求：

- a) 应具备与卫星、地面传感器、地质监测站，以及预报预警、灾害风险普查等合法数据源的对接功能；
- b) 应具备多源数据的融合分析能力，宜具备多维、多模态灾害数据的融合分析功能，实现对灾害风险因素的动态感知、早期识别与等级评估；
- c) 应具备灾害预警信息和防范建议的生成功能，给出预测结果提出防范措施与应对建议；
- d) 应具备对灾害预警响应效果的模拟与评估功能。

8.4.2 辅助应急处置

辅助应急处置应至少符合以下要求：

- a) 具备异常信号识别和评估功能，对采集数据中的异常信号进行识别和分类，并评估事件危害程度；
- b) 具备突发事件动态决策支持功能，提供情景模拟、应急资源需求分析、调度方案建议与应急指挥辅助等；
- c) 具备事件处置分析报告生成功能。

8.4.3 辅助政策评估

辅助政策评估应至少符合以下要求：

- a) 具备政策实施效果比对功能，基于关键指标，对比政策实施前与实施后的状态；
- b) 具备政策影响分析功能，对政策实施带来的社会影响、经济影响及环境影响等进行综合分析；
- c) 具备政策评估报告生成功能。

8.4.4 辅助评审

辅助评审应符合以下要求：

- a) 具备构建评审知识库与规则库功能；
- b) 具备待评审文件关键信息提取与结构化解析功能，依据相关法律法规、政策文件和标准规范要求，判断文件内容的合规性、合理性及可行性，并输出评审意见与改进建议；
- c) 具备评审报告生成功能，记录评审过程、专家意见和评审结果统计分析等。

9 安全合规要求

9.1 基本要求

安全合规基本要求如下：

- a) 应完成网信部门备案；
- b) 应符合 GB/T 45396、GB/T 45654、GB/T 45674、GA/T 2380 等相关国家标准和行业规定的规定；
- c) 应使用具有合法来源的数据和基础模型；
- d) 应采用大模型安全护栏等技术措施，识别拦截政务大模型应用输入输出中的重要数据泄露，提示词注入攻击，违法和不良信息等。

9.2 数据安全要求

数据安全应至少符合以下要求：

- e) 系统具备敏感信息识别拦截与动态更新功能；

- f) 系统具备政务数据额的全生存周期管控功能，包括权限控制、数据加密传输和加密存储等，应用 GB/T 32905、GB/T 32918、GB/T 32907 规定的商用密码算法。

9.3 模型和系统安全要求

模型和系统安全应至少符合以下要求：

- a) 模型具备幻觉处理能力，通过外挂知识库、事实核查等提高输出结果的准确性；
- b) 系统具备在关键节点决策与流程控制中引入人工干预的功能；
- c) 系统具备模型运行环境与推理过程的安全防护功能，包括攻击拦截溯源、推理依据与路径可视化、多租户资源隔离及权限控制等。

9.4 内容生成安全要求

内容生成安全应至少符合以下要求：

- a) 模型具备生成内容风险识别与校验功能，重点识别分析用户问题是否涉及 GB/T 45654—2025 附录 A 规定的安全风险，以及个人隐私、敏感舆情等内容；
- b) 模型具备对敏感信息、违法事项、越权请求等的拒答和引导功能。

9.5 监管审核要求

合规监管应至少符合以下要求：

- a) 系统具备全流程日志记录功能，包括用户提问、模型推理、结果输出及复核等全过程记录；
- b) 系统具备审核功能，审核并管控输出内容不超出业务范围和知悉范围。支持设置强制性人工审核节点，以适应高风险业务场景需要。

10 部署运维要求

10.1 系统部署

系统部署应至少符合以下要求：

- a) 模型产品和服务完成网信部门备案；
- b) 系统支持私有政务云或本地化部署；
- c) 系统具备模型热插拔功能，支持动态加载已完成训练的政务大模型；
- d) 系统具备流程可视化编排功能，支持通过拖拽式交互，完成办事流程的灵活组装与配置。

10.2 运维工具

运维工具至少符合以下要求：

- a) 应具备底层异构算力、存储、网络设备等资源统筹管理与调度功能；
- b) 应具备基础运维与容器编排调度功能；
- c) 应具备模型实例状态详情查询功能，查询状态信息包括实例状态、模型名称、模型版本、GPU 型号和数量等；
- d) 应具备综合监控与观测功能，构建统一监控视图，实现推理性能实时监控、全生存周期告警；
- e) 应具备故障自动检测与预设恢复策略执行功能，支持故障诊断留痕、服务重启、节点切换、版本回滚等，确保故障处置全程可追溯；
- f) 应具备异常诊断与故障根因分析功能，融合多维运维数据与智能算法，实现高效精准的故障定位与问题诊断；

- g) 应具备面向多角色的服务门户，提供应用程序编程接口（API），支撑跨部门、跨系统业务协同；
- h) 应具备运维权限分级管控能力，基于最小权限原则，划分运维人员的操作权限；
- i) 宜提供数据监控接口，监控数据同步至政务运维监管系统并可视化展示。

10.3 模型管理

模型管理应至少符合以下要求：

- a) 具备数据访问控制功能，对训练数据、微调数据、推理数据实施权限管理，限制模型调用者的操作范围；
- b) 具备模型安全防护功能，能抵御数据篡改、模型窃取、对抗样本攻击等；
- c) 具备向量数据库与政务知识库的集成功能，保障知识库数据高效赋能模型推理；
- d) 具备模型评估功能，从准确率、召回率、F1分数、模型总调用次数、模型调用失败次数、输入词元（input tokens）、输出词元（output tokens）、政策合规性、措辞严谨性、处理时效性等指标进行评估，并展示分析评估结果；
- e) 具备模型版本管理功能，记录模型的更新信息；
- f) 具备模型性能的持续监控和优化功能；
- g) 具备模型稳定性测试和验证功能；
- h) 具备模型日志记录功能，包括用户请求、原始输入、最终输出、安全事件、配置变更等信息。

10.4 系统管理

系统管理应至少符合以下要求：

- a) 具备用户管理、角色管理和授权管理等功能，确保不同层级的政务人员仅能访问其职责范围内的系统功能与数据资源；
- b) 具备对模型训练数据、推理数据的权限控制功能，能依据业务需求灵活配置数据访问策略，防止数据越权访问与滥用。

11 非功能性要求

11.1 可靠性要求

系统可靠性要求如下：

- a) 应提供不间断服务；
- b) 应具备故障检测、告警与自动恢复功能；
- c) 应具备服务多实例部署与弹性容错能力；
- d) 应建立数据备份与恢复机制；
- e) 应具备任务执行状态跟踪、异常提示与持续服务提供能力；
- f) 应具备过载控制能力。

11.2 兼容性要求

系统兼容性要求如下：

- a) 应适配政务领域数据格式、接口规范与编码要求；
- b) 应支持与政务信息系统和数据共享平台的对接、数据共享和功能联动。

11.3 维护性要求

系统维护性要求如下：

- a) 应具备操作行为、模型调用、数据访问的全程日志记录，并支持定期审计；
- b) 应具备运行监控与版本管理功能；
- c) 应提供标准格式接口，支持功能模块、基础大模型、算法插件、接口服务、知识资源的扩展；
- d) 应具备政务大模型、知识库的更新与同步功能；
- e) 应具备数据集规模、均衡性、标注质量对算法结果影响的分析功能；
- f) 应提供性能度量与验证方法，支持系统性能的持续评估；
- g) 应建立用户反馈机制，驱动模型持续优化；
- h) 应提供清晰的操作提示、异常说明与引导信息，常用功能宜支持便捷访问；
- i) 操作流程宜符合政务业务使用习惯。

参 考 文 献

- [1] 《政务领域人工智能大模型部署应用指引》
-